USING VMWARE AND LIVE CD’S TO CONFIGURE A SECURE, FLEXIBLE, EASY TO MANAGE COMPUTER LAB ENVIRONMENT

David Collins
Sam Houston State University, Huntsville, Texas
Center of Excellence in Digital Forensics, Department of Computer Science
(936) 294-3522
dcc002@shsu.edu

ABSTRACT
The task of managing a networked computer lab for class instruction is a daunting task at best. Most environments of this nature are not homogeneous, i.e. they must accommodate various software, operating systems, database applications, and security configurations. Each class or lab most likely requires a specific set of applications and software configurations tailored to the nature of the course. Managing this type of environment is difficult even with the client/server imaging software available today. VMWare is an elegant solution to this problem. VMWare is an x86 hardware abstraction layer that sits between the host hardware and the virtual operating system. The virtual operating system can be Windows XP, Windows 2003 Server, Red Hat Linux, Fedora Core, Sun, or any number of popular operating systems. These operating systems are installed on top of VMWare running on the host. By using VMWare to provide software, operating system, and networking support for multiple dissimilar computer courses, a lab manager can reduce her management burden significantly while increasing the security of the lab machines, minimizing configuration inconsistencies, and providing maximum flexibility to computer science instructors.
INTRODUCTION

Managing a networked computer lab used by numerous individuals can be a daunting task. Network managers are faced with configuration, security, application, and operating system specific issues on a daily basis. Every time a computer is used by an individual, it is difficult to determine if the computer is left in a stable desirable configuration. In addition, different class environments frequently require different software configurations. For instance, a class in digital forensics may require a completely different set of applications, operating systems, security settings and other configurations than would a class in network security. One option is to create images of each configuration and restore lab computers with the appropriate image depending on which class will be using them. This choice has some drawbacks in that the restore process can take considerable time depending on how large the image is and the speed of the network used to multicast the restore. This option is also clumsy when it comes to restoring different images simultaneously. Even if it were feasible to exclusively use images, we are limited to one operating system per machine at a time, i.e. we cannot support multiple simultaneously running operating systems. A better solution is to use VMWare in conjunction with imaging software like Norton Ghost to create an image of a flexible, secure system supporting multiple simultaneous software, operating system, and security configurations. Once this image is created, we can use imaging client/server software to restore all lab computers to the same state and use VMWare to select specific environments to run in, according to class requirements.

WHAT IS VMWARE?

Much like most computer science technology, VMWare technology is not a recent development. IBM developed CP 67 in 1967 to emulate the IBM 360, and more recently, it released IBM VM/370, a direct descendant of CP 67. [3][4] VMWare is similar in that it is a hardware abstraction or “layer” over the x86 architecture [1] that sits between an application and the system hardware (Figure 1). VMWare is very much like a generic kernel which can serve many flavors of operating systems including Windows XP, Windows 2003 Server, Red Hat Linux, Fedora Core, Mandrake Linux, and Sun Operating Systems, among others. These Operating systems are fully functional and run on top of VMWare. In other words, VMWare is not an operating system emulator. It is merely a hardware abstraction layer. This means that users of operating systems running on top of VMWare get the full benefit of the operating system and the host hardware without the side effects of running applications on the host! Using a traditional approach is problematic because we trade off security for flexibility. The more secure we make the systems the less we can do with them. Using a VMWare approach reduces the tradeoff in that we can create an ultra-secure host, and a virtual machine or machines which can run at any security level we wish. If the virtual machine breaks or becomes unstable, since it is merely an application, we can shut it down and restart it from a pre-saved snapshot and we are back to the state we started within a matter of seconds. This is regardless of changes in registry settings, system file changes, or any other changes to the state of the operating system. VMWare is a much more attractive option than restoring an image every time we need to revert to a particular state.
Multiple environments can be created and used with VMWare with the only real limitation being RAM. VMWare will support one virtual machine in addition to the host on 512 MB of RAM. Any additional virtual machines require more RAM in a linear fashion, i.e. 2 virtual machines will require approximately 1 GB RAM to run properly. Machines outfitted with 2 GB of RAM or more can support several virtual machines per host, and they provide excellent test beds for client server and distributed software development. Other scenarios include security training and incremental software development on multiple platforms. Developers can write and test software on multiple platforms without the need to reboot or repartition the host.[1] VMWare is available in several flavors including a client workstation edition and a server line[5].

Honeypotting is another use of VMWare in a lab environment. A honeypot is a computer system designed to be compromised. In fact its very value lies in the information gleaned from examining the compromised system. Valuable information can include statistics which provide insight into the patterns hackers follow[6].

**USING VMWARE IN THE LAB**

Security training can be facilitated by VMWare in a way that provides for security in the host network and flexibility in the virtual network. VMWare supports virtual switches which can connect virtual machines with each other, the host, physical machines, switches, routers, and firewalls on the host network. If your hosts are on a private network, then this option is very attractive for network security training and simulation. With only a few hosts, a network manager can simulate numerous clients and servers, each running the operating system and applications of choice with little if any security risk. When the next class arrives, we simply revert to our snapshot of choice, and within a few minutes we are set up for the new class. Another use of this product in the classroom is in Operating Systems Courses in a Computer Science Curriculum. These courses usually function at a theoretical level, and programming assignments generally
consist of scheduler simulators all running in user or unprivileged mode. To use kernel mode functionality over the course of developing an operating system is problematic because machines would need to be set aside for exclusive use by the developer during the code, test, reboot, and debug cycle. [1] This is inconvenient at best and expensive at worst. Using VMWare, we can write to the kernel API at will, save snapshots during the development cycle, and revert back to a particular state at any time. During this development process, other non-related courses can be taught on the same machine without interfering with the development process.

CREATING INSTRUCTIONAL MOVIES

Another VMWare feature that rates mentioning is its ability to record every event as it occurs in a virtual machine. VMWare can record events and save the events as a *.avi movie for playback at a later time. This functionality is an excellent option for instructors of computer science survey courses, integrated development environment courses, or any course that teaches students how to use a particular application. The traditional approach is to provide step by step instructions along with screen shots at each step to illustrate a process. This is clumsy because it is easy to leave out important steps or screenshots and students do not experience the flow of the process. Also, instructors many times use steps and screen shots from a book that may be out dated or missing information they feel is relevant to their course. With the recording functionality, students can play back a series of movies that the instructor created. This allows the student to get a more specific idea of the process, and she can follow along more easily. It also allows the instructor much more flexibility in that he can create these movies “on the fly” or with little preparation. If an instructor sees an alternate, better way of doing something, she can record the process and make it available to her class in short order. Many instructors write their own lab manuals and books for use in respective classes. These instructors could use VMWare to conveniently supply an accompanying CD in the lab manual with the various .avi files for the applications covered in the class.

CONFIGURING MULTIPLE LAB MACHINES USING GHOST AND LIVE BOOTABLE CD’S

Although VMWare is an excellent tool, it can be made more effective when used in conjunction with an imaging tool like Norton Ghost and “live” bootable CD’s. Ghost is a tool which creates a “copy” of a source disk or partition for restoration on single or multiple destination disks or partitions. GhostCast server supports the latter, and when used in concert with live bootable CD’s on the client machines, is an excellent solution to imaging multiple machines with a secure host and VMWare. A network manager would typically create an incremental library of images so that machines could be restored to any desired state at any time. For example, the network administrator could do a base install of the operating system which did not include updates, anti-virus, patches or service packs. We could revert to the base install in case of a virus infection during the installation process. We can incrementally image as we add updates, anti-virus software, etc. for the same reasons we save versions of software or other documents. One approach is to image the host with maximum security and VMWare as its only
application. The only software running on the host machine would be the host operating system, VMWare, and any software which directly supports security such as anti-virus software, updates, and service packs [2]. Once this is done, we can use one of the base images with updates, patches, and virus protection, but without VMWare and security templates applied, as a restore to the virtual machine instead of starting from scratch with the VM. This will speed the process up, and it will not require another Internet access for updates, thus minimizing our vulnerability to viruses during the update process.

CONCLUSION

As we have seen, VMWare is a tool which can reduce the management burden of the typical network administrator, provide for security in a test environment, provide an excellent test bed for software development, and it can make for an excellent teaching tool for application oriented classes. As computers and associated operating systems evolve, configuration becomes more and more complicated and burdensome. Any tools that ease that burden while increasing flexibility should be welcomed in our community. VMWare and Norton Ghost are two tools that do just that and should be considered for use by lab managers and instructors in all fields of study.

REFERENCES

1. Nieh, J., Can Leonard, O., Examining VMWare, Dr. Dobbs Journal, 2000
3. Murphey, R., Using VMWare for Forensics, 5th Annual Infragard Houston Members Alliance Fall Conference, 2005
5. Seifried, Kurt, Honeypotting with VMWare – Basics, http://www.seifired.org